The Skylar AI Platform

Version 2.4.0

Table of Contents

Introduction to Skylar AI **1**

What is Skylar AI? 2

Features of Skylar AI 2

Components of Skylar AI 2

Data Analyzed by Skylar AI 3

Configuring Skylar One for Skylar AI 4

Creating a Service Connection 4

Enabling Skylar AI for One or More Organizations 5

For Older Versions: Running the Skylar Management Tool 6

Enabling Skylar Analytics Event Policies 8

Configuring Skylar AI System Settings **10**

Logging In to the Skylar AI User Interface 11

Navigating the Skylar AI User Interface 11

Overview of Authentication in Skylar AI 12

Role-Based Access Control in Skylar AI 12

Elements of Role-Based User Accounts in Skylar AI 13

Configuring Multi-Factor Authentication 15

Configuring SSO Authentication with SAML 16

Additional Administrator and Account Features 17

Creating Access Tokens for Users 17

Configuring an IP Whitelist (Allow List) 18

Managing Dashboards in Skylar Analytics 19

Other Dashboard Options 19

Update All Datasets 20

Service Provider Administration for Skylar AI **21**

First Login as a Service Provider User 22

Provisioning a New Account 22

Adding an ODBC User 24

Chapter 1

Introduction to Skylar AI

Overview

Skylar AI is a software services suite powered by artificial intelligence (AI) that is designed to automatically manage and anticipate IT incidents. Skylar AI reasons over telemetry and the stored knowledge of an organization to deliver accurate insights, recommendations, and predictions.

Skylar AI includes Skylar Advisor or Skylar Analytics (or both), and Skylar Advisor currently requires Skylar Analytics. For more information, see the *Skylar AI Release Notes*.

The following table lists the minimum and recommended versions of ScienceLogic software required for Skylar AI and its components:

Product	Minimum Version	Recommended Version
Skylar One	*12.3.2*	*12.5.20 or later*
AP2	*8.18.43-81 (Jelly Bean)*	*9.13.1-14 (Quesito) or later*

This chapter covers the following topics:

What is Skylar AI? 2

Configuring Skylar One for Skylar AI 4

What is Skylar AI?

Autonomic IT leverages artificial intelligence (AI), automation, and data to intelligently self-manage an entire IT stack. Autonomic IT drives autonomous businesses with rapid decision-making, cost-optimized scalability, and innovative experiences that empower organizations to focus on core innovation. The Skylar AI platform, which includes Skylar Analytics and Skylar Advisor, helps customers with their journey towards Autonomic IT.

Skylar AI is a software services suite powered by artificial intelligence (AI) that is designed to automatically manage and anticipate IT incidents. Skylar AI reasons over telemetry and the stored knowledge of an organization to deliver accurate insights, recommendations, and predictions.

Skylar One collects data and leverages Skylar AI to learn the patterns for a particular device metric over a period of time. Skylar uses the resulting data to build a device metric-specific model that is used to define a scope of expected behavior as well as anomalous data points.

Features of Skylar AI

Skylar AI is the engine that powers several different software components. The components in the Skylar family of services share the following characteristics:

- **Reactive**. When something fails, Skylar AI tells you in plain language what happened and how to fix it with relevant context.
- **Predictive**. Skylar AI alerts you in advance to an expected out-of-capacity condition.
- **Proactive**. Skylar AI accurately answers any question asked of it with context drawn from company knowledge sources, such as bugs, support tickets, Knowledge Base articles, and Product Documentation, and recommends next steps.

Skylar AI integrates seamlessly with the Skylar One platform and other IT management tools. You can interact with Skylar AI through these familiar environments, where it enhances existing workflows with AI-driven insights and automation capabilities. Skylar AI can send you alerts and notifications, which can be customized to suit individual preferences or organizational needs. These alerts help you stay informed about potential issues, ongoing incidents, or opportunities for optimization.

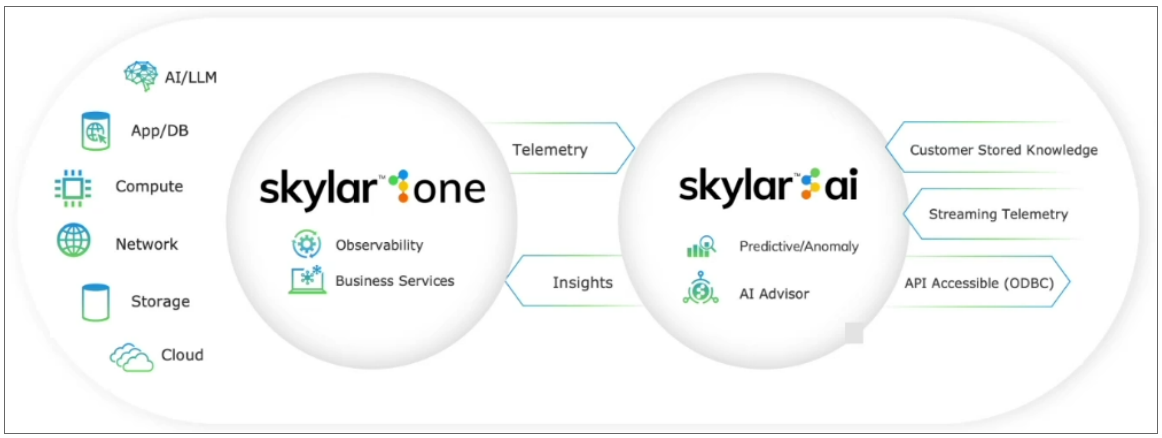
Components of Skylar AI

The Skylar AI family of services currently includes the following components:

- ***Skylar Advisor***, an AI-powered feature within the Skylar AI ecosystem that provides proactive, tailored guidance based on real-time data.
- ***Skylar Analytics***, an advanced reporting and custom analytics service that combines analytics with deep data exploration and visualization.

Data Analyzed by Skylar AI

The following image shows the flow of data into and out of Skylar One and Skylar AI:



The following list contains some of the types of data that Skylar One can send to the Skylar AI engine, where the data is analyzed and used by Skylar Advisor and Skylar Analytics:

- Alert and event logs
- Asset data
- Availability data
- Business services data, including owner organization ID; visible organization IDs; status; service policy name; and health, availability, and risk (HAR) refresh rate.
- Class-Based Quality-of-Service (CBQoS) metadata and CBQoS time series data
- Custom attributes for devices and for interfaces (interfaces require Skylar One version 12.3.14 or later, or Skylar One 12.5.4 or later)
- Device category and device group data
- DCM(+R) relationships and topology
- Dynamic Application mapping and performance data, and journals
- Email round-trip data
- Event data, including event policy names, information about an event's cleared status, the name and ID of the user who acknowledged the event, and event-related ticket information.
- Interface billing metrics, metadata, custom attributes, and tags
- Internal Collection processes, collection services, and CBQoS
- Journal Dynamic Application data
- Metadata for web content, SOAP/XML transactions, and domain name monitors
- Presentation objects, labels, and metrics collected by Dynamic Applications that include SNMP index collection objects
- Process and service data

- Skylar One Agent data, including Gen 1 (Skylar One Distributed Environment) and Gen 3 (Skylar One Extended Architecture) agents
- Thresholds
- Topology data for L2, L3, CDP, LLDP, and ad-hoc relationships between devices
- Windows service monitors and port monitors

Configuring Skylar One for Skylar AI

NOTE: If you or your site administrator needs to install Skylar AI in your environment, see *Installing and Configuring Skylar AI*.

Before you can start using Skylar AI components, you will need to perform the following configurations in Skylar One to enable the export of data from Skylar One to Skylar:

- *Create a Service Connection*
- *Enable Skylar Analytics for One or More Organizations*
- *Enabling Skylar AI Event Policies*

After you perform these configurations, you can access Skylar Analytics, Skylar Advisor, and other key Skylar AI components from the **Skylar AI**page ( ) in Skylar One.

A Skylar AI instance can ingest data from multiple external sources, but you should configure only a single Skylar One system to send data to that Skylar AI instance.

For information about setting up users, user groups, and user roles, see *Configuring Skylar AI System Settings*.

IMPORTANT: If you are connecting Skylar AI with a Skylar One system, ScienceLogic strongly recommends that you always use the most recent Skylar One and AP2 releases. Using the most recent releases will ensure that your Skylar AI system has access to the latest datasets and features. For more information, see the *Skylar One Platform Release Notes* and *Skylar One AP2 Release Notes*.

Creating a Service Connection

If you are using AP2 Mochi or later with your Skylar One system, you can create a service connection for the Skylar AI engine on the **Service Connections** page (Manage > Service Connections) in Skylar One. ScienceLogic strongly recommends upgrading to Mochi or later. For more information, see the *AP2 Mochi release notes*.

The service connection enables communication between your Skylar One system and Skylar AI. This process replaces the *Running the Skylar Management Tool* process in previous releases of Skylar Analytics and Skylar One.

To create a Skylar AI Engine service connection:

1. In Skylar One, go to the **Service Connections** page (Manage > Service Connections).
2. Click **Add Service Connection** and select *Skylar AI Engine*. The **Create Skylar AI Engine Credential** window appears.
3. Complete the following fields:
   - ***Name***. Type a name for the new service connection.
   - ***API Key***. Add the access token for Skylar AI, which you can generate on the **Access Tokens** page (> Account Settings > Instances > Access Tokens) in Skylar Settings. For more information, see *Creating Access Tokens for Users*.
   - ***Skylar AI Engine URL***. Add the URL for your Skylar AI system.
4. Click **[Save]**. The service connection is added to the **Service Connections** page, and a modal displays a link to the **Organizations** page, where you can enable Skylar Analytics for one or more organizations. See *Enabling Skylar AI for One or More Organizations* for more information.
5. Refresh or reload the browser to add all updates to Skylar One.

> **NOTE:** Newer releases of Skylar One include a ***Status*** and ***Status Updated*** column, along with a ***Service Check*** column that displays a **[Run Test]** button for "Skylar AI Engine" service connection types. Click **[Run Test]** to run a script to check the status of the Skylar AI connection and display the results in a modal.

Enabling Skylar AI for One or More Organizations

You will need to select one or more organizations in Skylar One that will share data with Skylar AI. This data will come from all of the devices in a selected organization. For a typical Skylar AI configuration, each Skylar One organization should match up with a distinct instance in the Skylar AI platform.

You can see which organizations are currently sending data to Skylar AI by going to the **Organizations** page (Registry > Accounts > Organizations) and looking at the ***Skylar AI Status*** column for the organizations. By default, the Skylar AI features are turned off.

To enable Skylar AI with Skylar One organizations:

1. In Skylar One, go to the **Organizations** page (Registry > Accounts > Organizations) and click the check box for one or more organizations.
2. In the ***Select Action*** field, select *Send Data from Selected Orgs to Skylar AI* and click **[Go]** to start sending data about the selected organizations to Skylar AI. The ***Skylar AI Status*** column for the selected organizations changes to *Enabled*.
3. If you want to override the hard-coded default options for exporting metadata to Skylar AI, you can add the JSON values in the ***Skylar Options (JSON)*** text field on the **Behavior Settings** page (System > Settings > Behavior). The values entered must be in the same JSON structure as those that appear in the **config.py** file:

```
DEFAULT_OPTIONS = { "metadata": { "intervals": {"snapshot": 60,
"cleared_events": 5}, "snapshot": { "batch_sizes": { "asset_basic":
500, "asset_ip_config": 10000, "perf_index_label": 5000, "device_
config": 20000, }, }, "cleared_events": { "query_range": 60, }, } }
```

NOTE: You can use the "Skylar: Failed" event policy in the "Skylar One Default Internal Events" PowerPack to raise an event in Skylar One if Skylar AI fails. If you installed Skylar One version 12.5.1 from an ISO file, this PowerPack will be included with the installation. If you are upgrading to Skylar One version 12.5.1, you will need to download the most recent "Skylar One Default Internal Events" PowerPack from the **PowerPacks** page on the ScienceLogic Support Center (Skylar One > PowerPacks) and then install the PowerPack.

NOTE: A generic, internal alert definition is generated in Skylar One to indicate whenever a Skylar AI connection is successful or encounters a problem.

For Older Versions: Running the Skylar Management Tool

If you are using a version of AP2 before Mochi, you will need to set up Skylar AI with the steps below for the Skylar SL1 Management Tool instead of the **Service Connections** page in Skylar One. ScienceLogic strongly recommends that you upgrade to Mochi. For more information, see the *AP2 Mochi release notes*.

The Management Tool configures Skylar One data and Skylar One processes, and it starts monitoring the Skylar connection and configuration. The script is named `sl-otelcol-mgmt.py`, and it is included in the `sl-otelcol` RPM package.

To run the Skylar SL1 Management Tool:

1. Use the following command to run the Management script on the Database Server (a Skylar One Central Database or a Skylar One Data Engine):

   ```
   sudo sl-otelcol-mgmt.py -vv skylar --skylar-all --skylar-endpoint "<URL_for_skylar_system>" --skylar-api-key "<skylar-access-token>" --ap2-feature-flags
   ```

   where:

   - `<URL_for_skylar_system>` is the URL for your Skylar AI system
   - `<skylar-access-token>` is the access token for Skylar AI, which you can generate on the **[Access Tokens]** tab of the **Skylar Settings** page. For more information, see *Creating Access Tokens for Users*.

   This command configures the OpenTelemetry Collector, restarts services that export data, and checks that connectivity to the supplied endpoints is healthy.

   You can also use the following configuration options if needed:

   - `--verify-cert false`. Allows users in on-premises environments to connect to Skylar AI using self-signed certificates.
   - `--ca-bundle /<path>/bundle.pem`. Allows users to specify a path to a **.pem** file and assign it to the `REQUESTS_CA_BUNDLE` environment variable.
   - `--skylar-disable`. Stops all Skylar AI exports and services. This flag performs the same operations as the pause command (see step 3, below) and also removes any Skylar AI pages from the Skylar One user interface.

NOTE: If you have already run setup before and are not changing the connection details, you do not need to include `--skylar-endpoint "<URL_for_skylar_system>" --skylar-api-key "<skylar-access-token>"`.

In addition, `--ap2-feature-flags` is only needed the first time you install Skylar AI.

   After successfully running the script, on the **System Logs** page (System > Monitor > System Logs), you will see "Info" messages for each configuration change (filter on `sl-otelcol-mgmt`). You will also see "Major" system log messages whenever connectivity fails for the Skylar endpoint or the OpenTelemetry Collector.

   After data streams into the Data Visualization dashboards, and other Skylar AI components, they will populate with data. Please note that this process might take several minutes.

2. If you have run the setup script before, run the following command to enable Skylar AI and make sure that everything is working as expected:

   ```
   sudo sl-otelcol-mgmt.py -vv skylar --skylar-all
   ```

3. If you need to pause Skylar AI, run the following command:

```
sudo sl-otelcol-mgmt.py -vv skylar
```

Pausing sets all Skylar AI toggle fields to disabled; restarts the event engine and data pull services to reflect the changed configuration; stops Skylar One managed services such as the Metadata Exporter, Alerts Poller, and **sl-otel-mgmt.timer**; and stops and disables the **sl-otelcol** systemd service.

4. To check the status of the installation, run the following command:

```
sudo sl-otelcol-mgmt.py -vv status
```

You should look for the following messages in the output:

```
---------- checking feature toggles
SL_EXPORT_EVENTS = False
SL_EXPORT_METRICS = True
SL_EXPORT_CONFIG = True
---------- checking services
sl-otelcol is enabled and running
---------- checking connectivity
checking: Skylar endpoint is healthy
checking: local OTELCOL endpoint is healthy
```

NOTE: If you need to turn off the Skylar AI connection, run the following command:

```
sudo sl-otelcol-mgmt.py -vv skylar --skip-status-service
```

5. Go to the previous procedure to specify the organizations you want to use for exporting data to Skylar.

Enabling Skylar Analytics Event Policies

In addition, the Predictive Alerting and Anomaly Detectioncomponents of Skylar Analytics require the "Skylar Analytics Event Policies" PowerPack. This PowerPack includes the Skylar One event policies from the "Skylar - Predictive events", "SL1: Skylar Anomaly Score Event Monitoring", and "SL1: Anomaly Index Event Monitoring" PowerPacks.

Older versions of this PowerPack were named "Skylar Predictive Analysis".

To install the "Skylar Analytics Event Policies" PowerPack:

1. Search for and download the PowerPack from the **PowerPacks** page at the ScienceLogic Support Center (Skylar One > PowerPacks, login required). Alternatively, you can use the link provided by ScienceLogic, if applicable.
2. In Skylar One, go to the **PowerPacks** page (System > Manage > PowerPacks), click **[Actions]**, and then click **[Import PowerPack]**.

3. Browse and select the downloaded PowerPack and click **[Import]**.
4. On the next screen, click **[Install]** and, when prompted for confirmation, click **[OK]**.
5. To confirm that the PowerPack was installed properly by go to the **Event Policies** page (Events > Event Policies) and type the word "predictive" into the ***Name*** search field. You should see a number of "Predictive Alerting" event policies.

The "Skylar Analytics Event Policies" PowerPack replaces the event policies in the following PowerPacks:

- Skylar Analytics
- Skylar - Predictive events
- SL1: Anomaly Score Event Monitoring
- SL1: Anomaly Index Event Monitoring

If you are still using event policies from those PowerPacks, ScienceLogic recommends that you complete the following steps to avoid disrupting existing events and Skylar AI links for predictive alerts:

1. In Skylar One, open each of the older PowerPacks on the **PowerPacks** page, go to the **Event Policies** tab, and click the remove or bomb icon () for each event policy to remove the older policies.
2. Import and install the latest "Skylar Analytics Event Policies" PowerPack.
3. Edit the "Skylar Analytics Event Policies" PowerPack and click the lightning icon () next to all of the event policies that start with "anom" or "pred" are aligned to the new PowerPack.
4. Delete the older PowerPacks.

NOTE: Going forward, upgrades and installs will not require you to repeat these steps.

Chapter 2

Configuring Skylar AI System Settings

Overview

This chapter covers how to configure the various settings for Skylar AI products by using the **Skylar Settings** page to update your user profile, edit the user interface theme, and specify your password and multi-factor authentication settings for Skylar AI.

You can also use the Skylar AI menu () at the top left of every page to access additional pages for the current Skylar AI application, along with User Settings and Account Settings for your Skylar AI applications.

The content in this chapter corresponds with the user interface for Skylar AI version 2.0.0 or later.

> **NOTE:** If you or your site administrator needs to install Skylar AI in your environment, see *Installing and Configuring Skylar AI*.

This chapter covers the following topics:

Logging In to the Skylar AI User Interface 11

Navigating the Skylar AI User Interface 11

Overview of Authentication in Skylar AI 12

Additional Administrator and Account Features 17

Logging In to the Skylar AI User Interface

If you know the URL of your Skylar AI system, you can go directly to that location. You can also access Skylar AI components from a link in Skylar One.

> **NOTE:** The login process might vary slightly, depending on the versions of Skylar AI, Skylar One, and the Skylar One AP2 user interface currently running in your environment.

To log in to Skylar AI from Skylar One:

1. From Skylar One, go to the **Skylar AI** page ( ) and click the **[Visit]** button for the Skylar AI component you want to use, such as Skylar Analytics or Skylar Advisor. If you are not currently logged in to Skylar AI, the Skylar AI sign-in page appears.
2. If you need to log in to Skylar AI, type your email address and password and click **[Continue]**. The Skylar AI landing page appears.
3. If your Skylar AI site requires multi-factor authentication, but you have not set it up, you will need to scan the QR code that displays or enter the "secret key". This is a one-time-only step.
4. Click the name of the Skylar AI component you want to use, such as ***Advisor***, ***Analytics***, or ***Skylar Settings***.

Navigating the Skylar AI User Interface

Use the following buttons and icons to help you navigate the Skylar AI user interface:

- The Skylar AI menu icon ( ) at top left gives you access to all of the pages for the current Skylar AI application, along with the **User Settings** page, the **Account Settings** pages, and the **Persona** page (Skylar Advisor only). The **User Settings** link takes you to the same **Profile** page that displays when you select ***Skylar Settings*** from the login page.
- Click the "Skylar AI" icon at top left to return to the Skylar AI login page.
- If you have multiple instances of Skylar AI running, you can switch between those instances by clicking the drop-down next to "Viewing Instance" at the top right.
- The user icon ( ) at top right displays the email address and role for the current user in the user interface. You can click the **[Sign Out]** button to sign out of this session.
- The notifications icon ( ) at the bottom left of the window lets you view all your recent notifications related to activities and warnings for that page. You can click **[Clear All]** to delete all past reminders. When you move to another page or tab, the list of notifications is updated for the new page.
- The **Versions** link in the footer of any page displays the version numbers for the current Skylar AI application. From the footer, you can also click links to view the Terms of Service and to view information about licenses and open-source packages.

Overview of Authentication in Skylar AI

Authentication for Skylar AI has the following features:

- Multi-tenant support, including a Super User login for host management .
- Multiple instances that represent separate domains of data access within an account (tenant).
- Pre-defined roles for access control.
- Email and password (local accounts) authorization by default, and Security Assertion Markup Language (SAML) single sign-on (SSO) authorization configured as needed.
- Access tokens for integration with external tools.

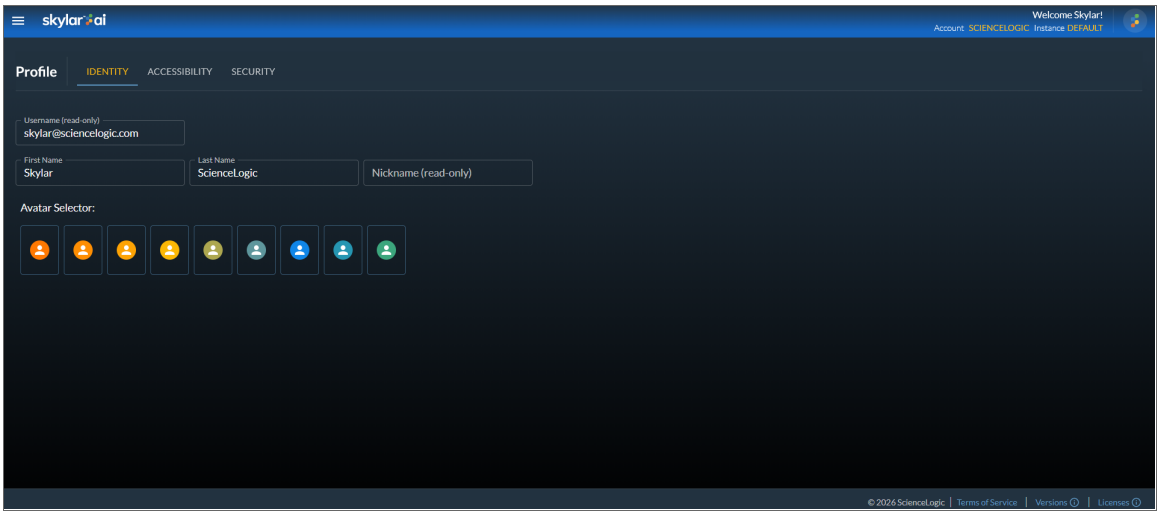
When a user is logged in to a Skylar AI component, that session uses the following rules:

- Email domains and SAML are configured per account (tenant).
- The first login for any new user starts with a prompt to create a new password.
- Logging into a user session requires either an email and password combination or a successful SAML2 redirect workflow.
- User passwords must be at least 15 characters long.
- New user passwords must be different from the last five passwords for this user.
- Users will be prompted to reset their passwords every 60 days.
- Users cannot change their passwords twice in 24 hours, and an error message displays if they try to do so.
- User sessions that have been idle for 15 minutes are automatically terminated. Administrator user sessions that have been idle for ten minutes are automatically terminated. An Admin user can adjust the timeout value on the **Authentication** page (> Account Settings > Account Access > Authentication).
- User accounts that have not been active for 35 days are automatically locked. Administrators can configure the inactivity timeout by using the ***Inactive User Timeout*** option on the **Authentication** page (> Account Settings > Account Access > Authentication).
- If a user has three failed login attempts within a 15-minute interval, the user's account is locked for 15 minutes. An administrator user can unlock that user account from the **Edit User** dialog on the **Users** page (> Account Settings > Account Access > Users).
- Account owners can log out all active users from the **Users** page (> Account Settings > Account Access > Users) by clicking **[Clear Active Users]**.

Role-Based Access Control in Skylar AI

To access the role-based access control settings, log into the Skylar AI user interface and click **Skylar Settings**. You can also access this page by going to the **User Settings** page (> User Settings).

The following image displays the **Profile** page in Skylar Settings:



Elements of Role-Based User Accounts in Skylar AI

An ***account*** in a Skylar AI system represents a complete Skylar AI configuration for a company. You can have multiple ***instances*** of Skylar AI in a single account.

An account contains a combination of the following:

- ***Instances***. An instance is a logical store for account data. In other words, an instance is a complete Skylar AI system with its own set of login credentials and user settings. Examples of instances include a production instance, a QA instance, and a testing instance. An account can contain multiple instances. A ***user*** can view only the instances that are specified on the ***groups*** to which that user is a member. If only one instance is available, you will use the instance labeled "default".

  On the **Available Instances** page (> Account Settings > Instances > Available Instances) in Skylar Settings , you can view a list of instances for the current user. An admin user can also access the ODBC connection information for an instance, which contains the Microsoft Open Database Connectivity (ODBC) host, password, port, and user information for Data Exploration using ODBC on the ODBC Users page (Analytics Admin > ODBC Users > ODBC Connection Info).

  If your system is using more than one instance, you will be able to select an instance after you log into Skylar Analytics.

- ***Access Tokens***. You can add access tokens to connect Skylar AI with Skylar One or a third-party application. The ***scope*** of an access token determines which application or service you can connect to with the access token. You can select more than one scope for an access token. You will need a different access token for each Skylar AI instance you are connecting to with an access token. You can set an expiration date for an access token, and you can also regenerate a token if needed.

  On the **Access Tokens** page (> Account Settings > Instances > Access Tokens) in Account Settings, you can view and add access tokens. For more information, see *Using Access Tokens for Users*.

- ***Users***. Everyone using Skylar AI should have their own user accounts. A user must belong to at least one ***group***.

  On the **Users** page (> Account Settings > Account Access > Users) in Account Settings, you can view, edit, and add users for an account, and you can also reset the password for a user.

- ***Groups***. A group controls which areas of Skylar AI a user can access. User groups are configured with a ***role*** and either a list of specific instances or *All* instances. If you select *All* instances, any instances that are created later are aligned with this group. Users can belong to more than one group. The active role for a user is based on the highest privilege from the groups aligned with that user.

  On the **Groups** page (> Account Settings > Account Access > Groups) in Account Settings, you can view, edit, and add user groups for an account.

- ***Roles***. A role controls what features a user can access. You assign a role by creating or editing a user, and then aligning a group to that user. The active role for a user is based on the highest privilege from the groups aligned with that user.

  The types of roles include the following:

  - **Super User**. Assigned to the **admin** user that can manage all user accounts. The default login is **skylar@sciencelogic.com**. The Super User role can create and manage customer accounts, manage multiple instances, and set up SAML authentication for a customer. A Super User has its own toolbar that displays at the top of the window in Skylar Settings, and you can expand or collapse this toolbar as needed.

  - **Service Provider**. This role lets you provision new accounts and set up SSO for accounts. This role cannot edit the user with the Super User role.

  - **Owner**. This role lets you monitor user management and user access, including the creation and assignment of instances. The **Owner** role also has the privilege to reset a user password.

  - **Admin**. This role lets you perform day-to-day configuration tasks, including integrations and customization. The **Admin** role has access to the **SQL Lab** page in Skylar Analytics, which gives the Admin user access to all of the data in the instance. An Admin user can also add, edit, and delete users.

  - **Editor**. For a future release, this role will let a user edit (create, update, and delete) objects, particularly incident type metadata.

    NOTE: For this release of Skylar AI, the **Editor** and **Viewer** roles are the same. In future releases, these roles will be further defined.

  - **Viewer**. For a future release, this role will give a user read-only access to Skylar AI. **Viewer** users can edit their own profiles.

- ***Authentication***. Each Skylar AI system is configured by the **Owner** user by default for email authentication, which uses an email address and password combination. An **Owner** user can also set up authentication with a shared Identity Provider through the SAML2 protocol. If you enable single sign-on (SSO) with SAML, users that log in with the specified domain will be redirected to the SAML provider for this account.

  On the **Authentication** page (> Account Settings > Account Access > Authentication), you can configure SAML for this account. For more information, see *Configuring SSO Authentication with SAML*.

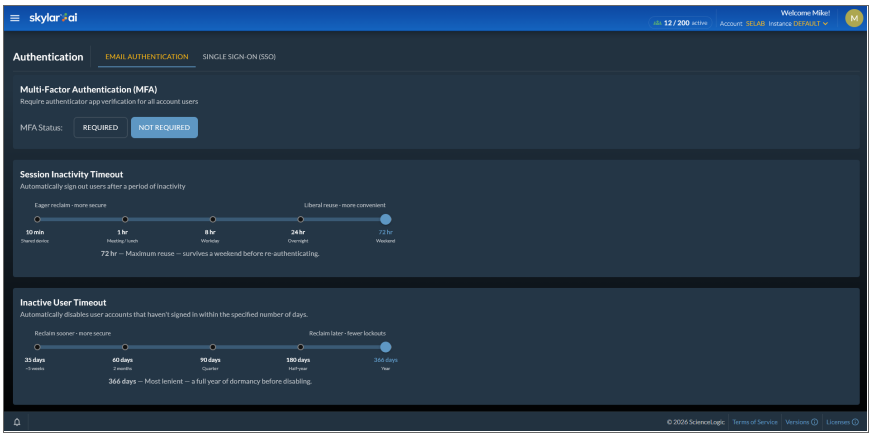
Configuring Multi-Factor Authentication

Skylar AI owner users can enable multi-factor authentication (MFA) for all users on a Skylar AI instance. On a site where MFA is required, users will need to scan a QR code or type in a secret key to set up MFA the next time they log in (if MFA is not already set up for their user accounts). Users will need to download an authenticator application like Google Authenticator or Authy to finish setting up MFA.

NOTE: MFA is set to Required by default for all new Skylar AI systems.

To require MFA for all users:

1. As an owner user, go to the **Authentication** page and go to the **[Email Authentication]** tab (> Account Settings > Account Access > Authentication > Email Authentication):



2. Click *Required* next to the ***MFA Status*** field. The **Require Multi-Factor Authentication** modal appears.
3. Click **[Require MFA]**. All account users will need to set up an authenticator app on their next sign-in.

Users on a Skylar AI instance that does not have MFA required can set MFA for their account:

1. If needed, click the "Skylar AI" icon at top left to return to the Skylar AI login page and switch to ***Skylar Settings***.

2. In Skylar Settings, go to the **[Security]** tab of the **Profile** page (User Preferences > Profile > Security).
3. Click the **[Configure MFA]** button.
4. Follow the instructions on the **Configure Multi-Factor Authentication** page to set up MFA.

> **TIP:** Current MFA users can click the **[Reconfigure MFA]** button on the **[Security]** tab of the **Profile** page to change their MFA settings.

5. An owner user can click the *Reset MFA* option for a user on the **Users** page (> Account Settings > Account Access > Users); for example, if a user loses his or her phone.

> **NOTE:** A Super User can turn off MFA for all other users on a Skylar AI instance.

Configuring SSO Authentication with SAML

Users with the **Owner** role can configure single sign-on (SSO) authentication with SAML for their accounts. When SSO authentication with SAML is enabled, all logins for that customer will be authenticated by the SAML identity provider, such as Auth0, Okta, or JumpCloud.

If you have an issue with authenticating, you can contact ScienceLogic to disable SAML for the account and potentially reset the owner's local (non-SAML) password if needed.

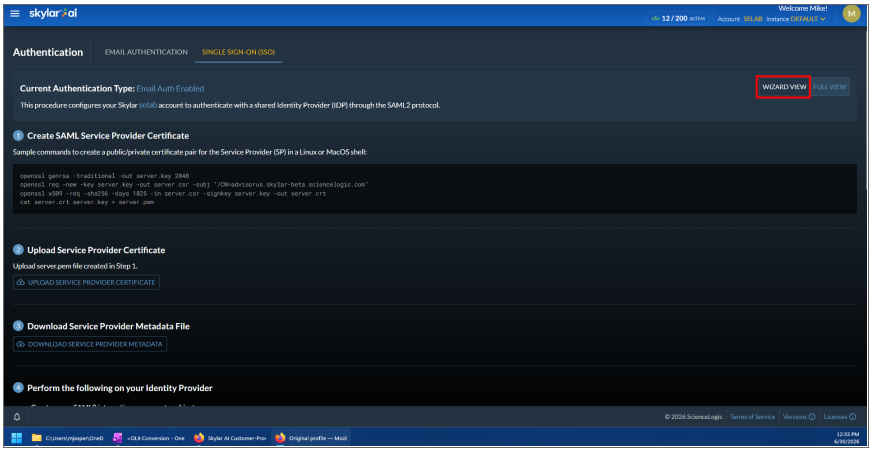
Before you can set up SSO authentication with SAML in Skylar AI, you will first need to create your user groups with your SAML identity provider if you do not already have them set up. Be sure to use the same names for your user groups with your SAML provider and with Skylar AI.

Do not switch the account to SAML until you have confirmed that the owner of the account has properly configured their SSO provider to recognize the Skylar platform.

To set up SSO Authentication with SAML in the Skylar AI user interface:

1. Go to the **Groups** page (> Account Settings > Account Access > Groups) in Account Settings and click **[Add Group]**. The **Add Group** dialog appears.
2. Type a name for the group, select a role of *Admin*, and select one or more instances.
3. Click **[Add]**. The group is added to the **Groups** page.

4. Go to the **Authentication** page (> Account Settings > Account Access > Authentication), click the **[Single Sign-On (SSO)]** tab, and review the instructions for SAML setup:



> **TIP:** You can click the **[Wizard View]** button to switch to a more step-by-step version of this configuration. The steps below are for the **[Full View]** option.

5. Follow steps 1-7 from the **[Single Sign-On (SSO)]** tab.

> **TIP:** For step 7 on the **[Single Sign-On (SSO)]** tab, after you click the **[Set Authentication Style]** button, you can select *Enable SAML Test Mode for 10 minutes* to test the new authentication configuration. If the authentication works as expected, you can come back to step 7 and select *SAML* to make the configuration permanent.

Additional Administrator and Account Features

This section covers the additional settings and features that you can access in Skylar Settings.

Creating Access Tokens for Users

You can use the **Access Tokens** page in Skylar Settings to add access tokens to connect Skylar AI with Skylar One or a third-party application. A Skylar access token is used for authentication in place of an API key.

You can set an expiration date for an access token, and you can also regenerate a token if needed.

To create an access token:

1. Log in to Skylar AI and go to the **Access Tokens** page (> Account Settings > Instances > Access Tokens).

2. Click the **[Add Access Token]** button. The **Add Access Token** window appears.
3. Complete the following fields:
    - ***Name***. Type a name for the token, such as "Skylar One Collector".
    - ***Scopes***. The scope of an access token determines which application or service you can connect to with the access token. You can select more than one scope for an access token. You will need a different access token for each Skylar AI instance you are connecting with access token. If you are creating this access token to *Create a Service Connection* in Skylar One , select both *sl1_connector* and *telemetry*.
    - ***Expiration Date***. Select an expiration date.
4. Click the **[Add]** button. The access token is added to the **Access Tokens** page.
5. Click the copy icon ( ) to copy the access token to the clipboard.

Configuring an IP Whitelist (Allow List)

On the **IP Whitelist** page in Skylar Settings, you can specify one or more source IP ranges to restrict access to your account to specific IP ranges. After you set up the IP whitelist, only IPs that are listed on this page will have access to the Skylar AI system.

If a user is having trouble logging in to Skylar AI, check this page to make sure that user's IP address is included in the allow list on this page. If this page is empty, all traffic to Skylar AI is allowed. As soon as one or more IPs are added, access is available to only those IP addresses.

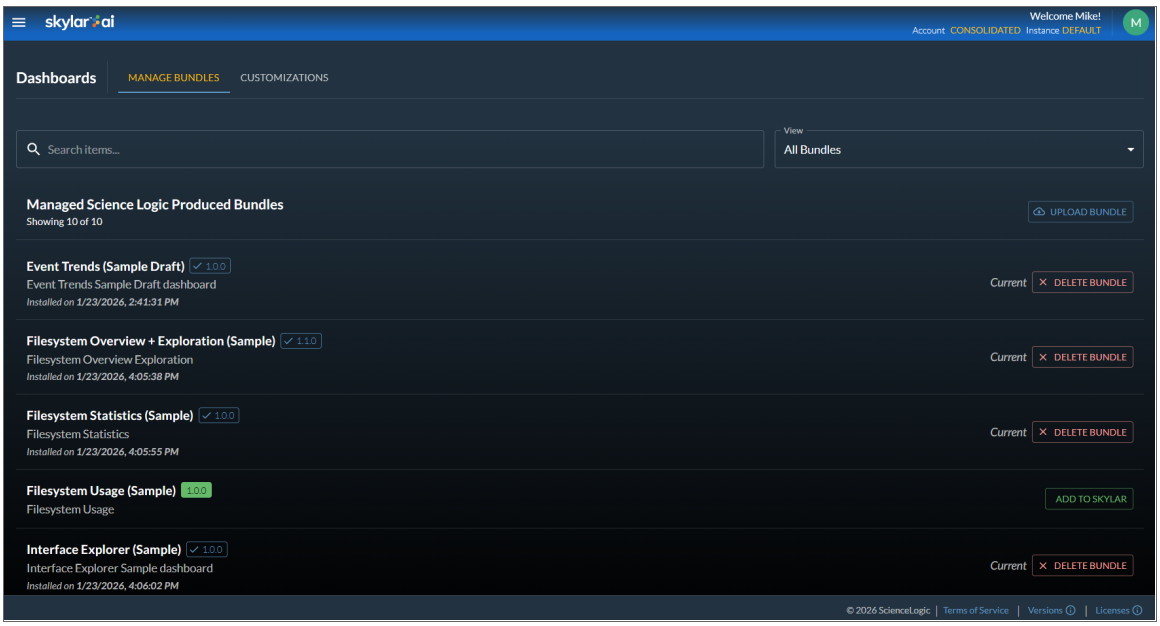
> **IMPORTANT:** Please note that this feature is different from the *whitelist (allow list) option for ODBC users* that is used when provisioning a new account.

To set up an IP allow list for Skylar AI:

1. Log in to Skylar AI and go to the **IP Whitelist** page (> Account Settings > Account Access > IP Whitelist).
2. Click the **[Add IP Range]** button. The **Add IP Range** window appears.
3. Complete the following fields to add IPs to the allow list:
    - ***Name***. Type a name for the IP range.
    - ***IP Range***. Enter the IP range in one of the following formats: 192.168.1.1, 192.168.0.0/24
4. Click **[Add]**.
5. Repeat steps 2-3 to add more IP ranges.

Managing Dashboards in Skylar Analytics

A user with an owner role can manage the Skylar Analytics dashboards on the **[Manage Bundles]** tab of the **Dashboards** page (> Analytics > Settings > Dashboard Mgmt):



You can search for dashboard bundles and sort the list of bundles by *All Bundles*, *Installed*, *Not Installed*, and *Updates Available*.

Owner users can install dashboards with **(Sample)** in their names by clicking the **[Add to Skylar]** button. These dashboards display a variety of visualization or chart configurations to show users different ways to display data, and users can reference these dashboards as examples. Many of the **(Sample)** dashboard layouts display multiple visualizations of the same raw data that would not typically be used at the same time on a production dashboard. These charts can also be copied and modified as needed, saving development time when building new dashboards.

ScienceLogic recommends that you keep the original versions of these **(Sample)** dashboard as unpublished draft dashboards and use them only for reference. For more information, see *Adding and Upgrading Dashboards*.

Other Dashboard Options

You have the following options on the **[Manage Bundles]** tab of the **Dashboards** page:

- **[Upload Bundle]**. Upload a .zip file containing a Skylar Analytics dashboard that has been exported from a Skylar Analytics system. This feature lets you share dashboards that were created and then exported by other users, for example.
- **[Add to Skylar]**. Click this button to install a new dashboard for Skylar Analytics

- **[Upgrade Now]**. Click this button to upgrade an existing dashboard. ***Current*** displays next to a dashboard to show that you are running the most recent version of that dashboard.
- **[Delete Bundle]**. Remove this bundle from the Skylar Analytics system.

Update All Datasets

In addition, you can use the **[Sync Skylar Datasets]** button on the **[Customizations]** tab on the **Dashboards** page to update all of your datasets based on Skylar One PowerPacks, including PowerPacks that have been updated in Skylar One.

If all datasets have been updated, the button does not appear, and the text "Datasets are current" appears instead. This button is only available to owner users in Skylar AI.

Appendix

A

Service Provider Administration for Skylar AI

Overview

This chapter explains the different tasks that a user with the **Service Provider** role can perform in Skylar AI. A **Service Provider** user can provision new accounts and add an ODBC user for the Data Exploration component of Skylar Analytics.

> **IMPORTANT:** This appendix is intended only for Skylar AI users with a role of **Service Provider**.

This chapter covers the following topics:

First Login as a Service Provider User 22

Provisioning a New Account 22

First Login as a Service Provider User

When you first log in to your Skylar AI system, you will use the default service provider name of **provider@sciencelogic.com**. The user interface will prompt you to set the ScienceLogic user password before your first login can continue.

After you log in for the first time, you will see a link for just the ***Skylar Settings*** page on the ***Skylar AI*** home page. Click that link to start setting up new accounts.

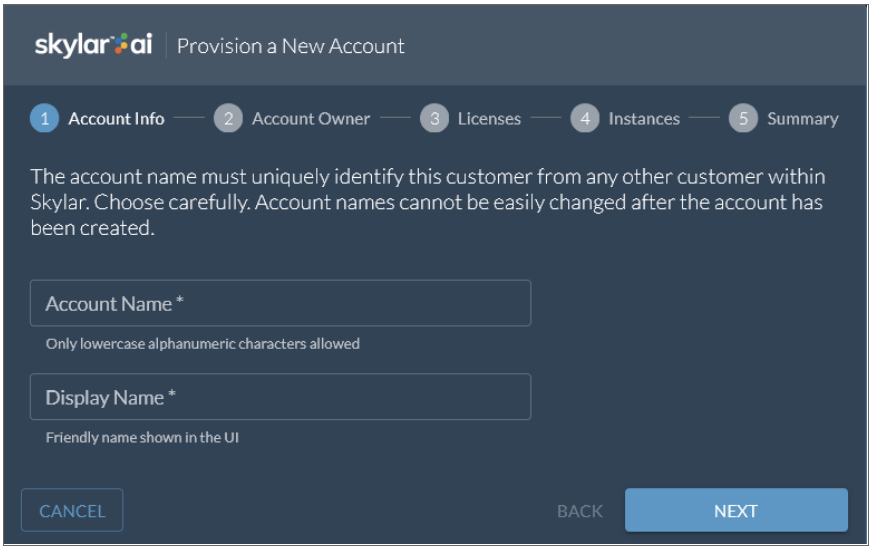
After you set up a licensed version of Skylar Analytics in Skylar Settings, you will see an ***Analytics*** link on this home page.

Provisioning a New Account

You can have multiple accounts in a single Skylar AI system. To add a new account, you will need to provision that account in Skylar Settings as a Super User.

To provision a new customer account:

1. Log in to Skylar AI as a Super User.
2. Click the ***All Accounts*** drop-down at the top of the page and select the customer account you want to provision. Skylar AI updates the contents of the page to show data for that account.
3. Click the ***All Accounts*** drop-down again and click **[Provision New Account]** at the bottom of the drop-down. The **Provision a New Account** wizard appears.



4. On the **Account Name** page, enter the name of the account in the ***Account Name*** field using only lower-case alphanumeric characters and type a user-friendly name for the account in the ***Display Name*** field.

5. Click **[Next]**.
6. On the **Account Owner** page, specify the ***First Name***, ***Last Name***, and ***Email*** for the first user of the new account.
7. When you enter an email address, Skylar AI automatically adds the domain name from that email to the ***Claim Email Domain*** field. If you are not using single sign-on (SSO) through Security Assertion Markup Language (SAML), or if you do not want to claim that email domain, you can remove the text from this field. This field is optional.

> **NOTE:** If you claim this domain, when SSO through SAML is enabled, users that log in with this domain will be redirected to the SAML provider for this account.

8. Click **[Next]**.
9. On the **Licenses** page, select ***Skylar Advisor*** if you want to enable Skylar Advisor for this account. You have the following additional options:
   - ***Enable Advisories***. Pairs Skylar Advisor to the data lake to mine telemetry to generate Advisories based on events and groups of similar events.
   - ***Legacy Instance ID***. For data lake connections, uses the legacy instance ID format.
   - ***Enable Organizations***. Restricts access based on organization. Once this feature is enabled, you will not be able to disable it.
10. Select ***Skylar Analytics*** to enable Skylar Analytics for this account. You have two additional options:
    - ***Consolidate Instance Reporting***. Enables reporting from multiple Skylar One systems on this Skylar AI system. When this option is enabled, data from all instances under the account will be merged into a single database called **reporting**.

      > **IMPORTANT:** You must enable this option during the account provisioning wizard, as you cannot change it or enable it after the wizard is complete. When enabled, a note indicating that consolidated instance reporting is active appears on the **Dashboards** page (> Analytics Admin > Dashboards) in Skylar Settings.

    - ***Enable ODBC***. Creates an ODBC connection for the Data Exploration component of Skylar Analytics. In the ***ODBC Client IP Ranges*** field, you will need to add the public-facing IP addresses for the ODBC client so those IP addresses are added to the whitelist or "allow list". Otherwise users will not be able to access the ODBC connection.

      These IP addresses display on the **ODBC Users** page (> Analytics > Settings > ODBC Users). For more information, see *Adding an ODBC User*.

      > **NOTE:** You will need to add your ODBC users on the **ODBC Users** page after you complete this procedure. For more information, see *Adding an ODBC User*.

11. Click **[Next]**.
12. On the **Instances** page, enter a name for the instance associated with this account using only lowercase alphanumeric characters. Examples include a production, QA, or testing instance. You can also use *default* as the instance name. Click **[Next]**.
13. On the **Summary** page, review your settings and click **[Begin Provisioning]** to continue setting up the account. The provisioning process starts, and Skylar AI switches to the new account.

> **NOTE:** When the account is set up, you will need to give the email address you used in step 7 to the first user. On first login, the new user will be prompted to change their password.

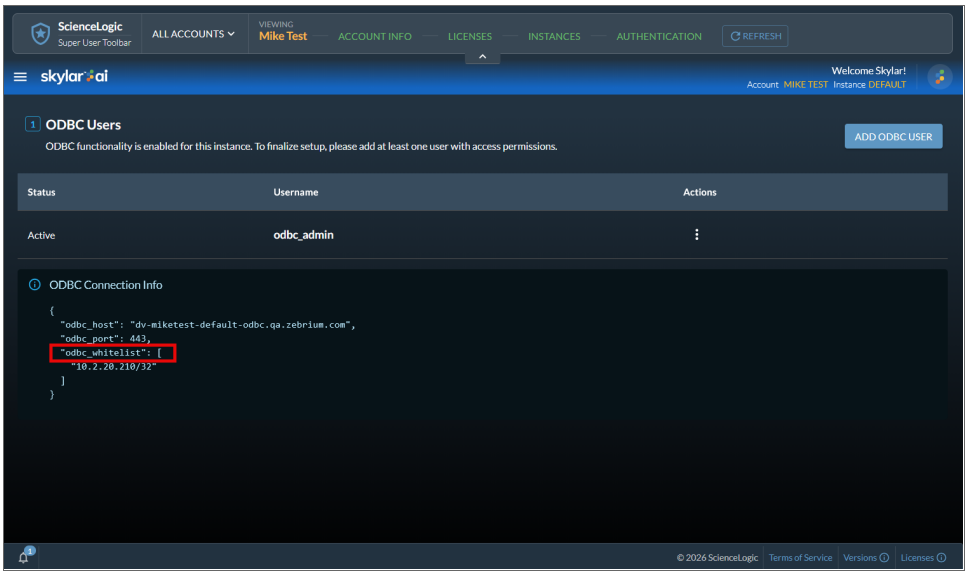
14. After the account is set up, you can use the following links on the Super User toolbar to further configure this account:
    - ***Account Info***. Lets you change the display name for this account.
    - ***Licenses***. Lets you change the Skylar Advisor and Skylar Analytics licensing options. These options are the same options as those in the steps above.
    - ***Instances***. Displays the current instances for this account, and lets you add another instance to the account.
    - ***Authentication***. Lets you select the type of authentication you want to use for this site: email/password or SAML. For more information, see *Configuring SSO Authentication with SAML*.
15. To set up other security and authentication settings, go to the **Authentication** page (> Account Settings > Account Access > Authentication). For more information, see *Configuring Skylar AI System Settings*.

Adding an ODBC User

If you (as a Super User) created a new ODBC connection for Skylar Analytics when you provisioned an account, you will need to create one or more ODBC users on the **ODBC Users** page in Skylar Settings. You can also edit or delete existing users on this page.

To add an ODBC user:

1. In Skylar Settings, go to the **ODBC Users** page (> Analytics > Settings > ODBC Users). This page displays the ODBC connection information for the Skylar AI system:



> **NOTE:** The IP address or addresses that display in the `"odbc_whitelist"` section of the code were *configured in the **Enable ODBC** field* on the **[Licenses]** tab as part of provisioning a new account. You cannot edit the addresses on this page, but you can edit them on the **[Licenses]** tab of the Super User toolbar.

2. Click the **[Add ODBC User]** button. The **Add ODBC User** window appears.
3. In the **Username** field, type a name after the "odbc_" prefix, and then type the password in the two **Password** fields.
4. Click the **[Add]** button. The ODBC user is added to the **ODBC Users** page.

© 2003 - 2026, ScienceLogic, Inc.

All rights reserved.

ScienceLogic™, the ScienceLogic logo, and ScienceLogic's product and service names are trademarks or service marks of ScienceLogic, Inc. and its affiliates. Use of ScienceLogic's trademarks or service marks without permission is prohibited.

ALL INFORMATION AVAILABLE IN THIS GUIDE IS PROVIDED "AS IS," WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED. SCIENCELOGIC™ AND ITS SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE OR NON-INFRINGEMENT.

Although ScienceLogic™ has attempted to provide accurate information herein, the information provided in this document may contain inadvertent technical inaccuracies or typographical errors, and ScienceLogic™ assumes no responsibility for the accuracy of the information. Information may be changed or updated without notice. ScienceLogic™ may also make improvements and / or changes in the products or services described herein at any time without notice.

800-SCI-LOGIC (1-800-724-5644)

International: +1-703-354-1010